ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Science of Computer Programming 51 (2004) 3–22

Science of Computer Programming

www.elsevier.com/locate/scico

Some results in dynamic model theory

Dexter Kozen*

Computer Science Department, Cornell University, Ithaca, NY 14853-7901, USA

Received 5 February 2003; received in revised form 17 April 2003; accepted 19 September 2003

Abstract

First-order structures over a fixed signature Σ give rise to a family of trace-based and relational Kleene algebras with tests defined in terms of *Tarskian frames*. A Tarskian frame is a Kripke frame whose states are valuations of program variables and whose atomic actions are state changes effected by variable assignments $x := e$, where e is a Σ-term. The Kleene algebras with tests that arise in this way play a role in dynamic model theory akin to the role played by Lindenbaum algebras in classical first-order model theory. Given a first-order theory T over Σ, we exhibit a Kripke frame U whose trace algebra Tr_U is universal for the equational theory of Tarskian trace algebras over Σ satisfying T, although U itself is not Tarskian in general. The corresponding relation algebra Rel_U is not universal for the equational theory of relation algebras of Tarskian frames, but it is so modulo observational equivalence.

MSC: 03B60; 03B70; 03G05; 03G15; 06E25; 03C05; 08A70; 08B20

Keywords: Model theory; Kleene algebra; Dynamic logic

1. Dynamic model theory

Traditional model theory [3,4], like classical predicate logic, is static in nature. Models, valuations of variables, and truth values of predicates are regarded as fixed and immutable. Dynamic model theory, on the other hand, is the study of abstract models in the presence of explicit operators that can change state. State change is typically effected by simple assignments $x := e$ and similar constructs that are explicit in the language. In addition, the language often provides various programming and data constructs for expressing high-level algorithmic properties of structures.

* Tel.: +1-607-255-9209; fax: +1-607-255-4428.
E-mail address: kozen@cs.cornell.edu (D. Kozen).

0167-6423/$ - see front matter
doi:10.1016/j.scico.2003.09.004

Dynamic model theory relates to dynamic logic and other programming logics as classical model theory relates to classical first-order logic. It has existed as a field of study almost as long as programming logics. One can find its roots in the early work of Andréka, Németi and Sain, Constable and O'Donnell, Engeler, Harel, Meyer, Mirkowska, Pratt, Salwicki, Stoulboushkin, Tiuryn, and many others; see [6] and references therein.

Dynamic model theory focuses on general algorithmic properties of first-order Tarskian structures, such as halting and equivalence of program schemes. Traditional model theory has had a profound influence on the development of the subject. For example, one interprets formulas and programs over first-order structures as in the Tarskian approach to the model theory of first-order logic. Perhaps the dominance of denotational over operational semantics in programming languages can be attributed to this influence as well.

However, there are some fundamental incompatibilities. For example, there are very simple and ubiquitous concepts in computer science, such as transitive closure, that cannot be expressed in first-order logic. Indeed, probably the single most important tool in reasoning about programs is induction, but first-order logic is incapable of handling it in general structures. In dynamic model theory, as programs and computation take on greater importance, the traditional first-order constructs $\forall$ and $\exists$ play a correspondingly lesser role.

In this paper, we continue the study begun in [1,12] of the general properties of trace-based and relational Kleene algebras with tests (KAT) that arise naturally from first-order structures. Such algebras are defined in terms of a specialized class of Kripke frames called *Tarskian frames*. A Tarskian frame is a Kripke frame whose states are valuations of program variables and whose atomic actions are state changes that arise from variable assignments $x := e$, where e is a term over some fixed first-order signature. The Kleene algebras with tests that arise in this way play a role in dynamic model theory comparable to the role played by Lindenbaum algebras (a particular subclass of Boolean algebras) in classical first-order model theory.

In this paper, we prove the following results. Let Σ be a fixed first-order signature. Given a first-order theory T over Σ, we exhibit a Kripke frame U whose trace algebra Tr_U is universal for the equational theory of Tarskian trace algebras over Σ satisfying T, although U itself is not Tarskian in general. The corresponding relation algebra Rel_U is not universal for the equational theory of relation algebras of Tarskian frames, but it is so modulo observational equivalence.

This paper is organized as follows. Sections 2 and 3 contain background material. In Section 2, we review the syntax of propositional and first-order (schematic) Kleene algebra with tests (KAT and SKAT, respectively). In Section 3, we review the various semantic interpretations of KAT and SKAT. At the propositional level, we recall the definitions of Kripke frames and relation and trace algebras. We discuss the guarded string model and its particular importance in the theory of KAT. We also discuss canonical homomorphisms and recall basic results on the equational theories of these models. At the first-order level, we recall the definition of Tarskian frames over a first-order signature Σ.

In Section 4, we introduce the universal frame U and develop some of its basic properties, including the notion of spectrum of a first-order structure. Many of these properties follow from more general propositional-level considerations, and we develop these tools in Section 5, including the notions of induced subframes, coherence, and autobisimulation, along with their algebraic consequences. The main theorem on the universality of U for trace algebras of Tarskian frames is stated in Section 4 and proved at the end of Section 5.

In Section 6 we turn to relation algebras. We show that the universality result of Section 4 does not hold for relation algebras of Tarskian frames. However, it does hold modulo observational equivalence. Again, these results follow from more general propositional considerations, which we develop in Section 7.

2. Syntax

Kleene algebra (KA) is the algebra of regular expressions. A Kleene algebra with tests (KAT) is a Kleene algebra with an embedded Boolean subalgebra. In this section we describe the language of propositional and first-order Kleene algebra with tests.

2.1. Propositional

Let P and B be disjoint sets of symbols called the *atomic actions* and *atomic tests*, respectively. *Tests* are Boolean expressions over B and *actions* are regular expressions over P and tests. Formally,

$$\begin{array}{lll} \text{tests} & \mathsf{b},\mathsf{c},\mathsf{d},\ldots & \mathsf{b} ::= \text{atomic tests} \mid \mathsf{b}{+}\mathsf{c} \mid \mathsf{b}\mathsf{c} \mid \bar{\mathsf{b}} \mid 0 \mid 1 \\ \text{actions} & \mathsf{p},\mathsf{q},\mathsf{r},\ldots & \mathsf{p} ::= \text{atomic actions} \mid \mathsf{p}{+}\mathsf{q} \mid \mathsf{p}\mathsf{q} \mid \mathsf{p}^* \mid \mathsf{b} \end{array}$$

The set of all actions over P and B and the set of all tests over B are denoted $\mathsf{RExp}_{\mathsf{P},\mathsf{B}}$ and $\mathsf{BExp}_{\mathsf{B}}$, respectively. Note that the latter is a subset of the former.

Ordinary programming constructs such as conditional tests and while loops can be encoded. For example, **while** b **do** p is $(\mathsf{b}\mathsf{p})^*\bar{\mathsf{b}}$. The Hoare partial correctness assertion $\{\mathsf{b}\}\ \mathsf{p}\ \{\mathsf{c}\}$ is expressed as an equation $\mathsf{b}\mathsf{p}\bar{\mathsf{c}} = 0$, or equivalently, $\mathsf{b}\mathsf{p} = \mathsf{b}\mathsf{p}\mathsf{c}$.

2.2. First order

For interpretations over first-order (Tarskian) structures, we refine the language of KAT to accommodate first-order terms and formulas. The resulting system is called schematic KAT (SKAT) [1].

Let Σ be a first-order signature consisting of function symbols $f, g, \ldots$ and relation symbols $P, Q, \ldots$, each with a fixed arity. We also have infinitely many individual first-order variables $x, y, \ldots$. Individual terms are denoted $d, e, \ldots$ and first-order formulas are denoted $\varphi, \psi, \ldots$.

In SKAT, atomic programs P are *assignments* $x := e$, where x is a variable and e is a Σ-term, and atomic tests B are atomic formulas $P(e_1, \ldots, e_n)$, where P is an n-ary relation symbol of Σ and $e_1, \ldots, e_n$ are Σ-terms.

The substitution operator that simultaneously substitutes a term d for all free occurrences of a variable x is denoted $[x/d]$. The substitution operator can be applied to

either terms or formulas, as in $e[x/d]$ or $\varphi[x/d]$. Bound variables in φ are implicitly renamed to avoid capture.

A *program scheme* is just an automaton over this language [11], which by a construction analogous to Kleene's theorem gives an equivalent expression in $\mathsf{RExp}_{\mathsf{P,B}}$. Using this idea, it is possible to give an alternative algebraic treatment of the theory of program schemes [1].

3. Semantics

3.1. Kleene algebra with tests

A *Kleene algebra with tests* (KAT) is a two-sorted structure $(K, B, +, \cdot, {}^*, \bar{}, 0, 1)$ such that

- $(K, +, \cdot, {}^*, 0, 1)$ is a Kleene algebra,
- $(B, +, \cdot, \bar{}, 0, 1)$ is a Boolean algebra, and
- $(B, +, \cdot, 0, 1)$ is a subalgebra of $(K, +, \cdot, 0, 1)$.

The Boolean complementation operator $\bar{}$ is defined only on B. Elements of B are called *tests*. These algebras were introduced in [9] and their theory and applications further developed in [1,2,5,10,11,13–15].

Boolean algebra has a well-known equational axiomatization; see for example [3,4]. Kleene algebra has a quasiequational axiomatization consisting of equations and equational implications. A *Kleene algebra* $(K, +, \cdot, *, 0, 1)$ is an idempotent semiring under $+, \cdot, 0, 1$ such that $\mathsf{p}^*\mathsf{q}$ is the $\leqslant$-least solution to $\mathsf{q} + \mathsf{px} \leqslant \mathsf{x}$ and qp^* is the $\leqslant$-least solution to $\mathsf{q} + \mathsf{xp} \leqslant \mathsf{x}$, where $\leqslant$ refers to the natural partial order $\mathsf{p} \leqslant \mathsf{q} \stackrel{\text{def}}{\Leftrightarrow} \mathsf{p} + \mathsf{q} = \mathsf{q}$. A Kleene algebra is *-*continuous* if it satisfies the stronger infinitary property $\mathsf{pq}^*\mathsf{r} = \sup_n \mathsf{pq}^n\mathsf{r}$.

Standard examples of Kleene algebras include the family of regular sets over a finite alphabet, the family of binary relations on a set, and the family of $n \times n$ matrices over another Kleene algebra. Other more exotic interpretations include the min,+ algebra or *tropical semiring* used in shortest path algorithms and models consisting of convex polyhedra used in computational geometry. All these models are *-continuous.

The axiomatization for KA above was proposed in [8], where it was shown that all true identities between regular expressions interpreted as regular sets of strings are derivable from the axioms of Kleene algebra. Equivalently, the algebra of regular sets of strings over the finite alphabet P is the free Kleene algebra on generators P. The axioms are also complete for the equational theory of relation algebras.

Analogous results exist for KAT, which we describe in Section 3.7 below. In addition, KAT is deductively complete for relationally valid propositional Hoare-style rules involving partial correctness assertions [10], whereas Hoare logic is not.

3.2. Kripke frames

For applications in program verification, one usually interprets programs and tests over a KAT consisting of sets of traces or sets of binary relations on a set of states.

Both these classes of algebras are defined in terms of *Kripke frames*. A Kripke frame over a set of atomic programs P and a set of atomic tests B is a structure $(K, \mathfrak{m}_K)$, where K is a set of *states*, $\mathfrak{m}_K : \mathsf{P} \to 2^{K\times K}$, and $\mathfrak{m}_K : \mathsf{B} \to 2^K$. The map $\mathfrak{m}_K$ specifies a canonical interpretation of the atomic actions and tests.

3.3. Relation algebras

The set of all binary relations on a Kripke frame K forms a KAT under the standard binary relation-theoretic interpretation of the KAT operators. The operator $\cdot$ is interpreted as relational composition $\circ$, $+$ as union, $\mathtt{0}$ and $\mathtt{1}$ as the empty relation and the identity relation on K, respectively, and * as reflexive transitive closure. The Boolean elements are subsets of the identity relation. This is called the *full relation algebra on* K. One can define a canonical interpretation $[\ \ ]_K : \mathsf{RExp}_{\mathsf{P},\mathsf{B}} \to 2^{K\times K}$ by

$$[\mathsf{p}]_K \stackrel{\text{def}}{=} \mathfrak{m}_K(\mathsf{p}), \quad \mathsf{p} \in \mathsf{P}$$
$$[\mathsf{b}]_K \stackrel{\text{def}}{=} \{(u,u) \mid u \in \mathfrak{m}_K(\mathsf{b})\}, \quad \mathsf{b} \in \mathsf{B}$$

extended homomorphically. A binary relation is *regular* if it is $[\mathsf{p}]_K$ for some $\mathsf{p} \in \mathsf{RExp}_{\mathsf{P},\mathsf{B}}$. The subalgebra consisting of all regular binary relations on K is denoted Rel_K.

3.4. Trace algebras

A *trace* in a Kripke frame K is a sequence $s_0\mathsf{p}_0 s_1 \cdots s_{n-1}\mathsf{p}_{n-1}s_n$, where $n \geqslant 0$, $s_i \in K$, $\mathsf{p}_i \in \mathsf{P}$, and $(s_i, s_{i+1}) \in \mathfrak{m}_K(\mathsf{p}_i)$ for $0 \leqslant i \leqslant n-1$. The set of all traces in K is denoted Traces_K. We denote traces by $\sigma, \tau, \ldots$. The first and last states of a trace σ are denoted $\mathsf{first}(\sigma)$ and $\mathsf{last}(\sigma)$, respectively. If $\mathsf{last}(\sigma) = \mathsf{first}(\tau)$, we can fuse σ and τ to get the trace $\sigma\tau$. If $\mathsf{last}(\sigma) \neq \mathsf{first}(\tau)$, then $\sigma\tau$ does not exist.

The powerset of Traces_K forms a KAT in which $+$ is interpreted as set union, $\cdot$ as the operation

$$AB \stackrel{\text{def}}{=} \{\sigma\tau \mid \sigma \in A,\ \tau \in B,\ \mathsf{last}(\sigma) = \mathsf{first}(\tau)\},$$

$\mathtt{0}$ and $\mathtt{1}$ as $\emptyset$ and K, respectively, and A^* as the union of all finite powers of A. The Boolean elements are the subsets of K, the sets of traces of length 0. This is called the *full trace algebra on* K. A canonical interpretation $[\![\ \ ]\!]_K$ for KAT expressions over P and B is given by

$$[\![\mathsf{p}]\!]_K \stackrel{\text{def}}{=} \{s\mathsf{p}t \mid (s,t) \in \mathfrak{m}_K(\mathsf{p})\}, \quad \mathsf{p} \in \mathsf{P}$$
$$[\![\mathsf{b}]\!]_K \stackrel{\text{def}}{=} \mathfrak{m}_K(\mathsf{b}), \quad \mathsf{b} \in \mathsf{B},$$

extended homomorphically. A set of traces is *regular* if it is $[\![\mathsf{p}]\!]_K$ for some KAT expression p. The subalgebra of all regular sets of traces of K is denoted Tr_K.

3.5. Guarded strings

When B is finite, a language-theoretic interpretation is given by the algebra of regular sets of *guarded strings* [7,14]. This algebra plays the same role in KAT that the algebra of regular sets of ordinary strings plays in KA.

Let $\mathsf{Atoms}_{\mathsf{B}}$ denote the set of atoms (minimal nonzero elements) of the free Boolean algebra generated by B. The symbols $\alpha, \beta, \ldots$ denote atoms. For an atom α and a test b, note that $\alpha \leqslant \mathsf{b}$ in the sense of KAT iff $\alpha \to \mathsf{b}$ is a propositional tautology.

A *guarded string* over P, B is a trace in the Kripke frame G whose states are $\mathsf{Atoms}_{\mathsf{B}}$ and

$$\mathfrak{m}_G(\mathsf{p}) \stackrel{\text{def}}{=} \mathsf{Atoms}_{\mathsf{B}} \times \mathsf{Atoms}_{\mathsf{B}}, \quad \mathsf{p} \in \mathsf{P}$$
$$\mathfrak{m}_G(\mathsf{b}) \stackrel{\text{def}}{=} \{\alpha \in \mathsf{Atoms}_{\mathsf{B}} \mid \alpha \leqslant \mathsf{b}\}, \quad \mathsf{b} \in \mathsf{B}.$$

Thus a guarded string is just a sequence $\alpha_0 \mathsf{p}_0 \alpha_1 \cdots \alpha_{n-1} \mathsf{p}_{n-1} \alpha_n$, where the $\alpha_i \in \mathsf{Atoms}_{\mathsf{B}}$ and $\mathsf{p}_i \in \mathsf{P}$, and Traces_G is the set of all guarded strings over P, B. Each KAT term $\mathsf{p} \in \mathsf{RExp}_{\mathsf{P},\mathsf{B}}$ denotes a set $[\![\mathsf{p}]\!]_G$ of guarded strings under the canonical interpretation defined in Section 3.4. A guarded string σ is itself a member of $\mathsf{RExp}_{\mathsf{P},\mathsf{B}}$, and $[\![\sigma]\!]_G = \{\sigma\}$.

The trace algebra Tr_G of regular sets of guarded strings over P, B forms the free Kleene algebra with tests on generators P, B; in other words, $[\![\mathsf{p}]\!]_G = [\![\mathsf{q}]\!]_G$ iff $\mathsf{p} = \mathsf{q}$ is a theorem of KAT [14].

3.6. Canonical homomorphisms

If K, K' are KATs with distinguished canonical interpretations $I : \mathsf{RExp}_{\mathsf{P},\mathsf{B}} \to K$ and $I' : \mathsf{RExp}_{\mathsf{P},\mathsf{B}} \to K'$, a homomorphism $h : K \to K'$ is *canonical* if it commutes with I and I'. In particular, a homomorphism involving trace or relation algebras on Kripke frames over P, B is canonical if it commutes with $[\![\ ]\!]_K$ and $[\ ]_K$.

An example of a canonical homomorphism is the map $\mathsf{Ext} : \mathsf{Tr}_K \to \mathsf{Rel}_K$ defined by

$$\mathsf{Ext}(A) \stackrel{\text{def}}{=} \{(\mathsf{first}(\sigma), \mathsf{last}(\sigma)) \mid \sigma \in A\}. \tag{1}$$

This is canonical because $\mathsf{Ext}([\![\mathsf{p}]\!]_K) = [\mathsf{p}]_K$ for all $\mathsf{p} \in \mathsf{RExp}_{\mathsf{P},\mathsf{B}}$ [15, Section 3.4].

Another important example is given by the following construction, which shows that every trace algebra is canonically isomorphic to a relation algebra. This construction is a straightforward generalization of a similar construction of [16] for regular sets of strings and [14] for regular sets of guarded strings.

Given a Kripke frame $(K, \mathfrak{m}_K)$, define a new Kripke frame $(R, \mathfrak{m}_R)$ with

$$R \stackrel{\text{def}}{=} \mathsf{Traces}_K$$
$$\mathfrak{m}_R(\mathsf{p}) \stackrel{\text{def}}{=} \{(\sigma, \sigma\tau) \mid \sigma\tau \in \mathsf{Traces}_K,\ \tau \in [\![\mathsf{p}]\!]_K\}, \quad \mathsf{p} \in \mathsf{P}$$
$$\mathfrak{m}_R(\mathsf{b}) \stackrel{\text{def}}{=} \{\sigma \in \mathsf{Traces}_K \mid \mathsf{last}(\sigma) \in [\![\mathsf{b}]\!]_K\}, \quad \mathsf{b} \in \mathsf{B}.$$

For $A \subseteq \mathsf{Traces}_K$, define

$$h(A) \stackrel{\text{def}}{=} \{(\sigma, \sigma\tau) \mid \sigma\tau \in \mathsf{Traces}_K,\ \tau \in A\}.$$

Lemma 3.1. *The map h is an injective* KAT *homomorphism from the full trace algebra 2^{Traces_K} to the full relation algebra $2^{R\times R}$. Its restriction to the regular trace algebra Tr_K is a canonical isomorphism $\mathsf{Tr}_K \to \mathsf{Rel}_R$.*

Proof. We show first that h is a homomorphism.

$$\begin{aligned} h\left(\bigcup_i A_i\right) &= \left\{(\sigma,\sigma\tau) \,\middle|\, \sigma\tau \in \mathsf{Traces}_K,\ \tau \in \bigcup_i A_i\right\} \\ &= \bigcup_i \{(\sigma,\sigma\tau) \mid \sigma\tau \in \mathsf{Traces}_K,\ \tau \in A_i\} \\ &= \bigcup_i h(A_i), \end{aligned}$$

$$\begin{aligned} h(AB) &= \{(\sigma,\sigma\tau\rho) \mid \sigma\tau\rho \in \mathsf{Traces}_K,\ \tau \in A,\ \rho \in B\} \\ &= \{(\sigma,\sigma\tau) \mid \sigma\tau \in \mathsf{Traces}_K,\ \tau \in A\} \\ &\quad \circ \{(\sigma\tau,\sigma\tau\rho) \mid \sigma\tau\rho \in \mathsf{Traces}_K,\ \rho \in B\} \\ &= h(A)h(B). \end{aligned}$$

The argument for * follows from these facts. For $B \subseteq K$,

$$\begin{aligned} h(\bar{B}) &= h(K - B) \\ &= \{(\sigma,\sigma\tau) \mid \sigma\tau \in \mathsf{Traces}_K,\ \tau \in K - B\} \\ &= \{(\sigma,\sigma) \mid \sigma \in \mathsf{Traces}_K,\ \mathsf{last}(\sigma) \in K - B\} \\ &= \{(\sigma,\sigma) \mid \sigma \in \mathsf{Traces}_K\} - \{(\sigma,\sigma) \mid \sigma \in \mathsf{Traces}_K,\ \mathsf{last}(\sigma) \in B\} \\ &= \{(\sigma,\sigma) \mid \sigma \in \mathsf{Traces}_K\} - \{(\sigma,\sigma\tau) \mid \sigma\tau \in \mathsf{Traces}_K,\ \tau \in B\} \\ &= \{(\sigma,\sigma) \mid \sigma \in \mathsf{Traces}_K\} - h(B) \\ &= \overline{h(B)}. \end{aligned}$$

The additive identities of 2^{Traces_K} and $2^{R\times R}$ are the empty set of traces and the empty relation, respectively, and

$$h(\emptyset) = \{(\sigma,\sigma\tau) \mid \sigma\tau \in \mathsf{Traces}_K,\ \tau \in \emptyset\} \quad = \quad \emptyset.$$

The multiplicative identities of 2^{Traces_K} and $2^{R\times R}$ are the set K and the identity relation on R, respectively, and the argument for this case follows from the above two facts.

The function h is injective, since A is uniquely recoverable from $h(A)$:

$$A = \{\tau \mid (\mathsf{first}(\tau), \tau) \in h(A)\}.$$

To show that the restriction of h to Tr_K is canonical, it suffices to show that h acts canonically on atomic symbols; that is,

$$h(\llbracket \mathsf{p} \rrbracket_K) = [\![\mathsf{p}]\!]_R, \quad \mathsf{p} \in \mathsf{P},$$
$$h(\llbracket \mathsf{b} \rrbracket_K) = [\![\mathsf{b}]\!]_R, \quad \mathsf{b} \in \mathsf{B}.$$

We have

$$\begin{aligned} h(\llbracket \mathsf{p} \rrbracket_K) &= \{(\sigma, \sigma\tau) \mid \sigma\tau \in \mathsf{Traces}_K,\ \tau \in \llbracket \mathsf{p} \rrbracket_K\} \\ &= \mathfrak{m}_R(\mathsf{p}) \\ &= [\![\mathsf{p}]\!]_R, \end{aligned}$$

$$\begin{aligned} h(\llbracket \mathsf{b} \rrbracket_K) &= \{(\sigma, \sigma\tau) \mid \sigma\tau \in \mathsf{Traces}_K,\ \tau \in \llbracket \mathsf{b} \rrbracket_K\} \\ &= \{(\sigma, \sigma) \mid \sigma \in \mathsf{Traces}_K,\ \mathsf{last}(\sigma) \in \llbracket \mathsf{b} \rrbracket_K\} \\ &= \{(\sigma, \sigma) \mid \sigma \in \mathfrak{m}_R(\mathsf{b})\} \\ &= [\![\mathsf{b}]\!]_R. \qquad \square \end{aligned}$$

3.7. Coincidence of the equational theories

The completeness theorem of [14] says that the guarded string algebra Tr_G and its associated canonical interpretation $\llbracket\ \rrbracket_G$ are *universal* for Kleene algebras with tests in the sense that for any KAT K and interpretation $I : \mathsf{RExp}_{\mathsf{P},\mathsf{B}} \to K$, there is a homomorphism $h : \mathsf{Tr}_G \to K$ that commutes with $\llbracket\ \rrbracket_G$ and I. In particular, the free KAT $(\mathsf{RExp}_{\mathsf{P},\mathsf{B}}/\equiv, \mathsf{BExp}_{\mathsf{B}}/\equiv)$ on generators P, B, where $\equiv$ is provable equivalence, is canonically isomorphic to Tr_G. This says that $\mathsf{p} = \mathsf{q}$ in all Kleene algebras with tests if and only if $\llbracket \mathsf{p} \rrbracket_G = \llbracket \mathsf{q} \rrbracket_G$.

In addition, the equational theory of KAT is the same as the equational theories of trace algebras and relation algebras [14]. Since Tr_G is universal, its equational theory is contained in the equational theories of trace algebras and relation algebras; and the reverse inclusions follow from the fact that Tr_G is itself a trace algebra and canonically isomorphic to a relation algebra by Lemma 3.1.

3.8. Tarskian frames

At the first-order level, we are primarily interested in interpretations over Kripke frames of a special form defined with respect to first-order structures $\mathfrak{A}$ of signature Σ. Such frames are called *Tarskian*. A state of a Tarskian frame is a map $s : \{x, y, \ldots\} \to |\mathfrak{A}|$ assigning a value to each variable. Such maps are commonly called *valuations* in logic and model theory and *environments* in computer science. These maps extend to terms and formulas inductively in the usual way, thus we may

consider a valuation s variously as a function $s : \{\text{terms}\} \to |\mathfrak{A}|$ or $s : \{\text{formulas}\} \to \{0,1\}$. We write $s \vDash \varphi$ if $s(\varphi) = 1$.

The action of the assignment $x := e$ is to change the state in the following way. The expression e is evaluated in the input state and the value assigned to x, and the resulting valuation is the output state. To define this formally, we define $s[x/a]$ to be the valuation that agrees with s everywhere except possibly at x, where it takes value a:

$$s[x/a](x) \stackrel{\text{def}}{=} a,$$
$$s[x/a](y) \stackrel{\text{def}}{=} s(y), \quad y \text{ different from } x.$$

Then the behavior of the assignment $x := e$ is to take state s to state $s[x/s(e)]$.

The unary operator $[x/a]$ on states is called a *rebinding operator*. It is not to be confused with the substitution operator, although its appearance is (intentionally) similar. There is a fundamental relationship between substitution and rebinding: for any term or formula E,

$$s[x/s(e)](E) = s(E[x/e]). \tag{2}$$

This is easily proved by induction on the structure of E.

Given a first-order structure $\mathfrak{A}$ of signature Σ, we can now define the Tarskian frame $(K_{\mathfrak{A}}, \mathfrak{m}_{\mathfrak{A}})$ as follows:

$$K_{\mathfrak{A}} \stackrel{\text{def}}{=} \{\text{valuations over } \mathfrak{A}\}$$
$$\mathfrak{m}_{\mathfrak{A}}(x := e) \stackrel{\text{def}}{=} \{(s, s[x/s(e)]) \mid s \in K_{\mathfrak{A}}\}$$
$$\mathfrak{m}_{\mathfrak{A}}(P(e_1, \ldots, e_n)) \stackrel{\text{def}}{=} \{s \in K_{\mathfrak{A}} \mid s \vDash P(e_1, \ldots, e_n)\}.$$

The Tarskian frame $K_{\mathfrak{A}}$ is just a Kripke frame, and as such gives rise to a regular relation algebra $\mathsf{Rel}_{\mathfrak{A}}$ and a regular trace algebra $\mathsf{Tr}_{\mathfrak{A}}$ as described in Sections 3.3 and 3.4. The set of all traces is denoted $\mathsf{Traces}_{\mathfrak{A}}$. The canonical interpretations associate sets $[\![\mathsf{p}]\!]_{\mathfrak{A}}$ and $[\![\![\mathsf{p}]\!]\!]_{\mathfrak{A}}$ of pairs and traces, respectively, with the term p.

We are interested in the specialized structure of trace and relation algebras of Tarskian frames as an algebraic representation of first-order program schemes. Note that a trace in $K_{\mathfrak{A}}$ is a sequence $s_0\mathsf{p}_0 s_1 \cdots s_{n-1}\mathsf{p}_{n-1}s_n$, where $s_{i+1} = s_i[x_i/s_i(e_i)]$ if p_i is the assignment $x_i := e_i$, $0 \leqslant i \leqslant n-1$. Thus a trace is uniquely determined by its start state and its sequence of atomic actions.

4. Universal frames

The importance and usefulness of the guarded string model in propositional KAT motivates us to seek a similar structure that plays the same role for the class of Tarskian models and SKAT. We propose the following definition.

4.1. Quantifier-free types

Let T be a fixed first-order theory of signature Σ (consistent set of first-order sentences closed under entailment). A *quantifier-free type* (qf-type) is a maximal consistent set of quantifier-free formulas. A *qf-type of* T is a qf-type consistent with T. Quantifier-free types are the natural analog of the atoms of B in the guarded string model.

Define the Kripke frame $(U, \mathfrak{m}_U)$ by

$$\begin{aligned} U &\stackrel{\text{def}}{=} \{\text{qf-types of } T\} \\ \mathfrak{m}_U(x := e) &\stackrel{\text{def}}{=} \{(\Delta, \{\varphi \mid \varphi[x/e] \in \Delta\}) \mid \Delta \in U\} \\ \mathfrak{m}_U(P(e_1, \ldots, e_n)) &\stackrel{\text{def}}{=} \{\Delta \in U \mid P(e_1, \ldots, e_n) \in \Delta\}. \end{aligned}$$

For the definition of $\mathfrak{m}_U(x := e)$ to make sense, the set $\{\varphi \mid \varphi[x/e] \in \Delta\}$ had better be a qf-type of T whenever Δ is. We argue this below (Corollary 4.2).

We will ultimately show that Tr_U is universal for trace algebras of Tarskian frames over models of T. Unlike the propositional case, however, this is not true for relation algebras. However it is almost true in a sense to be made precise in Section 6. The frame U itself is not isomorphic to any Tarskian frame in general.

Let $\mathfrak{A}$ be a model of T. For any valuation s over $\mathfrak{A}$, there is a unique qf-type $\Delta(s)$ such that $s \vDash \Delta(s)$. Note that $\Delta(s) \in U$, since any qf-type realized in a model of T is consistent with T.

Lemma 4.1. *$\Delta(s[x/s(e)]) = \{\varphi \mid \varphi[x/e] \in \Delta(s)\}$. In other words, the following diagram commutes*:

$$\begin{array}{ccc} s & \xrightarrow{\quad x := e \quad} & s[x/s(e)] \\ \Delta\downarrow & & \downarrow\Delta \\ \Delta(s) & \xrightarrow[\quad x := e \quad]{} & \Delta(s[x/s(e)]) \end{array} \quad = \{\varphi \mid \varphi[x/e] \in \Delta(s)\}$$

Proof. This is essentially a restatement of the relationship between substitution and rebinding (2). □

Corollary 4.2. *If $\Delta \in U$, then $\{\varphi \mid \varphi[x/e] \in \Delta\} \in U$.*

Proof. Suppose $\Delta \in U$. Let $\mathfrak{A}$ be a model of T realizing the type Δ, say $\Delta = \Delta(s)$. By Lemma 4.1, $\{\varphi \mid \varphi[x/e] \in \Delta\} = \Delta(s[x/s(e)]) \in U$. □

Now extend the map $\Delta : K_{\mathfrak{A}} \to U$ to traces

$$\Delta(s_0 \mathsf{p}_0 s_1 \cdots s_{n-1} \mathsf{p}_{n-1} s_n) \stackrel{\text{def}}{=} \Delta(s_0)\mathsf{p}_0\Delta(s_1) \cdots \Delta(s_{n-1})\mathsf{p}_{n-1}\Delta(s_n).$$

Lemma 4.3. *For any trace σ of $K_{\mathfrak{A}}$, the sequence $\Delta(\sigma)$ is a trace of U.*

Proof. We need to only argue that for any state s, $(\Delta(s), \Delta(s[x/s(e)])) \in \mathfrak{m}_U(x := e)$. This is immediate from Lemma 4.1 and the definition of $\mathfrak{m}_U$. □

By Lemma 4.3, we may consider Δ to be a map $\Delta : \mathsf{Traces}_{\mathfrak{A}} \to \mathsf{Traces}_U$. Now for $A \subseteq \mathsf{Traces}_U$, define

$$\Delta^{-1}(A) \stackrel{\text{def}}{=} \{\sigma \in \mathsf{Traces}_{\mathfrak{A}} \mid \Delta(\sigma) \in A\}.$$

Our main theorem is the following.

Theorem 4.4. *Δ^{-1} is a canonical* KAT *homomorphism $\mathsf{Tr}_U \to \mathsf{Tr}_{\mathfrak{A}}$. Moreover, Tr_U is* universal *for the equational theory of Tarskian trace algebras over models of T in the following sense. For all* p,q, $[\![\mathsf{p}]\!]_U = [\![\mathsf{q}]\!]_U$ *if and only if* $[\![\mathsf{p}]\!]_{\mathfrak{A}} = [\![\mathsf{q}]\!]_{\mathfrak{A}}$ *for all models $\mathfrak{A}$ of T.*

Theorem 4.4 will follow from some fairly general considerations, which we will develop in Section 5. We thus defer the proof of Theorem 4.4 until the end of that section.

4.2. Spectra

Let $\mathfrak{A}$ be a model of T. Define the *spectrum* of $\mathfrak{A}$ to be the set of qf-types realized in $\mathfrak{A}$:

$$\mathsf{spec}\,\mathfrak{A} \stackrel{\text{def}}{=} \{\Delta(s) \mid s \in K_{\mathfrak{A}}\}.$$

Then $\mathsf{spec}\,\mathfrak{A} \subseteq U$, since every qf-type realized in $\mathfrak{A}$ is consistent with T. The set $\mathsf{spec}\,\mathfrak{A}$ is the image of $K_{\mathfrak{A}}$ in U under Δ and gives an induced subframe

$$\mathfrak{m}_{\mathsf{spec}\,\mathfrak{A}}(x := e) \stackrel{\text{def}}{=} \mathfrak{m}_U(x := e) \cap (\mathsf{spec}\,\mathfrak{A})^2$$
$$\mathfrak{m}_{\mathsf{spec}\,\mathfrak{A}}(P(\bar{e})) \stackrel{\text{def}}{=} \mathfrak{m}_U(P(\bar{e})) \cap \mathsf{spec}\,\mathfrak{A}.$$

Theorem 4.5. *The map $\Delta^{-1} : \mathsf{Tr}_{\mathsf{spec}\,\mathfrak{A}} \to \mathsf{Tr}_{\mathfrak{A}}$ is a canonical isomorphism.*

Like Theorem 4.4, Theorem 4.5 holds under quite general conditions. These conditions can be stated and proved in a purely propositional framework, so we again defer the proof until after we have developed the requisite tools.

5. Constructions on Kripke frames

In this section, we develop the machinery that will be used in the proof of Theorems 4.4 and 4.5.

5.1. Induced subframes

Let $(L, \mathfrak{m}_L)$ be a Kripke frame and let K be a subset of L. The *induced subframe on* K is $(K, \mathfrak{m}_K)$, where

$$\mathfrak{m}_K(\mathsf{b}) \stackrel{\text{def}}{=} \mathfrak{m}_L(\mathsf{b}) \cap K, \quad \mathsf{b} \in \mathsf{B} \tag{3}$$

$$\mathfrak{m}_K(\mathsf{p}) \stackrel{\text{def}}{=} \mathfrak{m}_L(\mathsf{p}) \cap K^2, \quad \mathsf{p} \in \mathsf{P}. \tag{4}$$

We say that a binary relation R on L *preserves* K if $t \in K$ whenever $s \in K$ and $(s,t) \in R$.

Lemma 5.1. *Let* $(K, \mathfrak{m}_K)$ *be an induced subframe of* $(L, \mathfrak{m}_L)$ *such that all atomic actions* $\mathfrak{m}_L(\mathsf{p})$ *preserve* K.

(a) *The map* $A \mapsto A \cap \mathsf{Traces}_K$ *for* $A \subseteq \mathsf{Traces}_L$ *is a canonical* KAT *homomorphism* $\mathsf{Tr}_L \to \mathsf{Tr}_K$.
(b) *The map* $A \mapsto A \cap K^2$ *for* $A \subseteq L^2$ *is a canonical* KAT *homomorphism* $\mathsf{Rel}_L \to \mathsf{Rel}_K$.

Proof. (a) To show that $A \mapsto A \cap \mathsf{Traces}_K$ is a homomorphism with respect to the KAT operations, it suffices to show that $(\bigcup_i A_i) \cap \mathsf{Traces}_K = \bigcup_i (A_i \cap \mathsf{Traces}_K)$, $(A \cap \mathsf{Traces}_K)(B \cap \mathsf{Traces}_K) = AB \cap \mathsf{Traces}_K$, and for $A \subseteq L$, $(L - A) \cap \mathsf{Traces}_K = K - (A \cap \mathsf{Traces}_K)$. These arguments are all straightforward.

The map is canonical on Tr_L since it is a homomorphism and since it acts canonically on atomic symbols; that is, $[\![\mathsf{p}]\!]_L \cap \mathsf{Traces}_K = [\![\mathsf{p}]\!]_K$ and $[\![\mathsf{b}]\!]_L \cap \mathsf{Traces}_K = [\![\mathsf{b}]\!]_K$. These two equations are immediate from (3) and (4).

(b) The relations on L that preserve K form a sub-KAT of the full relation algebra on L. Moreover, if all atomic actions $\mathfrak{m}_L(\mathsf{p})$ preserve K, then this algebra contains Rel_L as a subalgebra. To show that $A \mapsto A \cap K^2$ is a homomorphism of this algebra with respect to the KAT operations, it suffices to show that $(\bigcup_i A_i) \cap K^2 = \bigcup_i (A_i \cap K^2)$, $(A \cap K^2)(B \cap K^2) = AB \cap K^2$, and for A a subset of the identity relation on L, $(\{(u,u) \mid u \in L\} - A) \cap K^2 = (\{(u,u) \mid u \in L\} - A) \cap K^2 = \{(u,u) \mid u \in K\} - (A \cap K^2)$. These arguments are all straightforward except for the inclusion $AB \cap K^2 \subseteq (A \cap K^2)(B \cap K^2)$, which is the only case that uses the assumption regarding the preservation of K. We argue this case explicitly.

$$\begin{aligned}
&(s,t) \in AB \cap K^2 \\
&\quad \Rightarrow \exists u \in L \ (s,u) \in A, \ (u,t) \in B, \ s,t \in K \\
&\quad \Rightarrow \exists u \in K \ (s,u) \in A, \ (u,t) \in B, \ s,t \in K \qquad \text{since } A \text{ preserves } K \\
&\quad \Rightarrow \exists u \ (s,u) \in A \cap K^2, \ (u,t) \in B \cap K^2 \\
&\quad \Rightarrow (s,t) \in (A \cap K^2)(B \cap K^2).
\end{aligned}$$

Again, $A \mapsto A \cap K^2$ is canonical on Rel_L since it is a homomorphism and by (3) and (4) acts canonically on atomic symbols; that is, $[\mathsf{p}]_L \cap K^2 = [\mathsf{p}]_K$ and $[\mathsf{b}]_L \cap K^2 = [\mathsf{b}]_K$. □

Lemma 5.2. *Let $\mathscr{C}$ be a collection of induced subframes of a frame L whose union covers L such that each subframe in $\mathscr{C}$ is preserved under atomic actions $\mathfrak{m}_L(\mathsf{p})$. Then Tr_L is universal for the equational theory of $\{\mathsf{Tr}_K \mid K \in \mathscr{C}\}$ and Rel_L is universal for the equational theory of $\{\mathsf{Rel}_K \mid K \in \mathscr{C}\}$ in the sense that*

(i) $[\![\mathsf{p}]\!]_L = [\![\mathsf{q}]\!]_L \Leftrightarrow$ *for all* $K \in \mathscr{C}$, $[\![\mathsf{p}]\!]_K = [\![\mathsf{q}]\!]_K$,
(ii) $[\mathsf{p}]_L = [\mathsf{q}]_L \Leftrightarrow$ *for all* $K \in \mathscr{C}$, $[\mathsf{p}]_K = [\mathsf{q}]_K$.

Proof. For (i), if $[\![\mathsf{p}]\!]_L = [\![\mathsf{q}]\!]_L$, then $[\![\mathsf{p}]\!]_K = [\![\mathsf{q}]\!]_K$ for all $K \in \mathscr{C}$, since there is a canonical homomorphism $\mathsf{Tr}_L \to \mathsf{Tr}_K$ by Lemma 5.1(a). Conversely, if $[\![\mathsf{p}]\!]_L \neq [\![\mathsf{q}]\!]_L$, say $\sigma \in [\![\mathsf{q}]\!]_L - [\![\mathsf{p}]\!]_L$, then since $\bigcup \mathscr{C}$ covers L, there exists $K \in \mathscr{C}$ such that $\mathsf{first}(\sigma) \in K$. Since the atomic actions $\mathfrak{m}_L(\mathsf{p})$ preserve K, σ is a trace of K. Then $\sigma \in [\![\mathsf{q}]\!]_L \cap \mathsf{Traces}_K = [\![\mathsf{q}]\!]_K$ but $\sigma \notin [\![\mathsf{p}]\!]_K \subseteq [\![\mathsf{p}]\!]_L$.

The proof of (ii) is similar. □

Note that $\mathsf{spec}\,\mathfrak{A}$ is an induced subframe of U, and if $\mathsf{spec}\,\mathfrak{A} \subseteq \mathsf{spec}\,\mathfrak{B}$, then $\mathsf{spec}\,\mathfrak{A}$ is an induced subframe of $\mathsf{spec}\,\mathfrak{B}$.

5.2. Coherence

Let K, L be Kripke frames over P, B. A function $f : K \to L$ is said to be *coherent* if

(i) $(s,t) \in \mathfrak{m}_K(\mathsf{p}) \Rightarrow (f(s), f(t)) \in \mathfrak{m}_L(\mathsf{p}), \quad \mathsf{p} \in \mathsf{P}$;
(ii) $s \in \mathfrak{m}_K(\mathsf{b}) \Leftrightarrow f(s) \in \mathfrak{m}_L(\mathsf{b}), \quad \mathsf{b} \in \mathsf{B}$.

Condition (i) implies that f can be extended to traces $f : \mathsf{Traces}_K \to \mathsf{Traces}_L$:

$$f(s_0\mathsf{p}_0 s_1 \cdots s_{n-1}\mathsf{p}_{n-1}s_n) \stackrel{\text{def}}{=} f(s_0)\mathsf{p}_0 f(s_1) \cdots f(s_{n-1})\mathsf{p}_{n-1}f(s_n).$$

This is essentially the property that we needed of Δ in the proof of Lemma 4.3. The function f is said to be *onto on traces* if its extension $f : \mathsf{Traces}_K \to \mathsf{Traces}_L$ is onto.

For a coherent function $f : K \to L$ and $A \subseteq \mathsf{Traces}_L$, define

$$f^{-1}(A) \stackrel{\text{def}}{=} \{\sigma \in \mathsf{Traces}_K \mid f(\sigma) \in A\}.$$

Lemma 5.3. *If $f : K \to L$ is coherent, then f^{-1} is a* KAT *homomorphism on the full trace algebras of K and L, and its restriction to the regular trace algebra Tr_L is a canonical homomorphism $\mathsf{Tr}_L \to \mathsf{Tr}_K$. If in addition f is onto on traces, then f^{-1} is one-to-one, therefore $f^{-1} : \mathsf{Tr}_L \to \mathsf{Tr}_K$ is a canonical isomorphism.*

Proof. First, we check that f^{-1} is a KAT homomorphism. It follows easily from elementary set-theoretic arguments that f^{-1} commutes with the Boolean operations and maps L to K. For concatenation, since $f(\tau\rho) = f(\tau)f(\rho)$,

$$\begin{aligned}\sigma \in f^{-1}(AB) &\Leftrightarrow f(\sigma) \in AB \\ &\Leftrightarrow \exists\tau\ \exists\rho \quad \sigma = \tau\rho,\ f(\tau) \in A,\ f(\rho) \in B\end{aligned}$$

$$\Leftrightarrow \exists\tau\ \exists\rho \quad \sigma = \tau\rho,\ \tau \in f^{-1}(A),\ \rho \in f^{-1}(B)$$
$$\Leftrightarrow \sigma \in f^{-1}(A)f^{-1}(B).$$

The case of the operator * follows from these cases.

To show that f^{-1} restricted to Tr_L is canonical, it suffices to show that it acts canonically on atomic symbols; that is,

$$f^{-1}(\llbracket \mathsf{p} \rrbracket_L) = \llbracket \mathsf{p} \rrbracket_K, \quad \mathsf{p} \in \mathsf{P},$$
$$f^{-1}(\llbracket \mathsf{b} \rrbracket_L) = \llbracket \mathsf{b} \rrbracket_K, \quad \mathsf{b} \in \mathsf{B}.$$

This amounts to showing that for all $s, t \in K$,

$$((s,t) \in \mathfrak{m}_K(\mathsf{p}) \text{ and } (f(s), f(t)) \in \mathfrak{m}_L(\mathsf{p})) \Leftrightarrow (s,t) \in \mathfrak{m}_K(\mathsf{p}), \quad \mathsf{p} \in \mathsf{P},$$
$$f(s) \in \mathfrak{m}_L(\mathsf{b}) \Leftrightarrow s \in \mathfrak{m}_K(\mathsf{b}), \quad \mathsf{b} \in \mathsf{B}$$

which are exactly properties (i) and (ii) in the definition of coherence.

Finally, we show that f^{-1} is one-to-one whenever f is onto on traces. If $A, B \subseteq \mathsf{Traces}_L$ and $A \neq B$, say with $A - B \neq \emptyset$, then since f is onto on traces, there exists a trace σ of K such that $f(\sigma) \in A - B$. Then $\sigma \in f^{-1}(A - B) = f^{-1}(A) - f^{-1}(B)$, therefore $f^{-1}(A) \neq f^{-1}(B)$. □

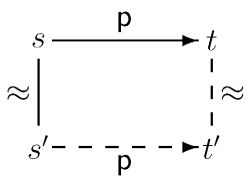
5.3. Autobisimulation

By Lemma 5.3, in order to prove Theorem 4.5, it will suffice to argue that the map $\Delta : K_{\mathfrak{A}} \to \mathsf{spec}\,\mathfrak{A}$ is coherent and onto on traces. For the latter property, we establish a general sufficient condition based on the notion of *bisimulation*.

For a coherent f to be onto on traces, the original $f : K \to L$ must be onto, since each single state of L is a trace. Assuming that this is true, every trace of L is of the form $f(s_0)\mathsf{p}_0 f(s_1) \cdots f(s_{n-1})\mathsf{p}_{n-1} f(s_n)$. We need to be able to construct a trace $s'_0\mathsf{p}_0 s'_1 \cdots s'_{n-1}\mathsf{p}_{n-1}s'_n$ of K such that $f(s'_i) = f(s_i)$. This will be possible when the function f is obtained from an *autobisimulation*.

An equivalence relation $\approx$ on K is called an *autobisimulation* if it satisfies the following two properties:

(i) For $\mathsf{b} \in \mathsf{B}$, if $s \approx s'$ and $s \in \mathfrak{m}_K(\mathsf{b})$, then $s' \in \mathfrak{m}_K(\mathsf{b})$.
(ii) For $\mathsf{p} \in \mathsf{P}$, if $s \approx s'$ and $(s,t) \in \mathfrak{m}_K(\mathsf{p})$, then there exists t' such that $(s',t') \in \mathfrak{m}_K(\mathsf{p})$ and $t \approx t'$.



The $\approx$-equivalence class of s is $[s] \stackrel{\text{def}}{=} \{t \mid s \approx t\}$. Given an autobisimulation $\approx$ on K, one can define a *quotient frame* $(K/\approx, \mathfrak{m}_{K/\approx})$ as follows:

$$
\begin{aligned}
K/\approx &\stackrel{\text{def}}{=} \{[s] \mid s \in K\} \\
\mathfrak{m}_{K/\approx}(\mathsf{b}) &\stackrel{\text{def}}{=} \{[s] \mid s \in \mathfrak{m}_K(\mathsf{b})\}, \quad \mathsf{b} \in \mathsf{B} \\
\mathfrak{m}_{K/\approx}(\mathsf{p}) &\stackrel{\text{def}}{=} \{([s],[t]) \mid (s,t) \in \mathfrak{m}_K(\mathsf{p})\}, \quad \mathsf{p} \in \mathsf{P}.
\end{aligned}
$$

Lemma 5.4. *Let $\approx$ be an autobisimulation on K with equivalence classes $[\ ]$. The map $[\ ] : K \to K/\approx$ is coherent and onto on traces, therefore $[\ ]^{-1} : \mathsf{Tr}_{K/\approx} \to \mathsf{Tr}_K$ is a canonical isomorphism.*

Proof. By Lemma 5.3, it suffices to check that the map $[\ ] : K \to K/\approx$ is coherent and onto on traces. It is easy to check that it is coherent and onto on single states. Now suppose we are given a trace

$$[s_0]\,\mathsf{p}_0\,[s_1]\cdots[s_{n-1}]\,\mathsf{p}_{n-1}\,[s_n]$$

of $K/\approx$. We wish to find $s'_0,\ldots,s'_n$ such that $s'_0\mathsf{p}_0 s'_1\cdots s'_{n-1}\mathsf{p}_{n-1}s'_n$ is a trace of K and $s'_i \approx s_i$, $0 \leqslant i \leqslant n$. By the definition of $\mathfrak{m}_{K/\approx}(\mathsf{p})$, for each i, $0 \leqslant i \leqslant n-1$, there exist s''_i and s'''_{i+1} such that $(s''_i, s'''_{i+1}) \in \mathfrak{m}_K(\mathsf{p}_i)$, $s''_i \approx s_i$, and $s'''_{i+1} \approx s_{i+1}$. We construct s'_i by induction on i. To start, take $s'_0 = s_0$. Now suppose we have constructed a prefix of the desired trace ending with s'_i such that $s'_i \approx s_i$. Then $s'_i \approx s''_i$. By property (ii) of autobisimulations, there exists s'_{i+1} such that $(s'_i, s'_{i+1}) \in \mathfrak{m}_K(\mathsf{p}_i)$ and $s'_{i+1} \approx s'''_{i+1} \approx s_{i+1}$. We have extended the trace by one step and maintained the invariant $s'_i \approx s_i$. □

At this point we are ready to prove our main theorems.

Proof of Theorem 4.5. Let $K_{\mathfrak{A}}$ be a Tarskian frame over a model $\mathfrak{A}$ of T. Checking the conditions of coherence for the map $\Delta : K_{\mathfrak{A}} \to U$, we observe that

(i) $(s,t) \in \mathfrak{m}_{\mathfrak{A}}(x := e) \Rightarrow (\Delta(s), \Delta(t)) \in \mathfrak{m}_U(x := e)$, since $\Delta(s[x/s(e)]) = \{\varphi \mid \varphi[x/e] \in \Delta(s)\}$ by Lemma 4.1; and
(ii) $s \in \mathfrak{m}_{\mathfrak{A}}(P(\bar{e})) \Leftrightarrow P(\bar{e}) \in \Delta(s)$ by definition of $\mathfrak{m}_{\mathfrak{A}}(P(\bar{e}))$.

By Lemma 5.3, $\Delta^{-1} : \mathsf{Tr}_U \to \mathsf{Tr}_{\mathfrak{A}}$ and $\Delta^{-1} : \mathsf{Tr}_{\mathsf{spec}\,\mathfrak{A}} \to \mathsf{Tr}_{\mathfrak{A}}$ are canonical homomorphisms. Moreover, by Lemma 4.1, the relation $s \approx t \stackrel{\text{def}}{\Leftrightarrow} \Delta(s) = \Delta(t)$ is an autobisimulation, and the quotient frame $K_{\mathfrak{A}}/\approx$ is isomorphic to $K_{\mathsf{spec}\,\mathfrak{A}}$, therefore by Lemma 5.4, $\Delta^{-1} : \mathsf{Tr}_{\mathsf{spec}\,\mathfrak{A}} \to \mathsf{Tr}_{\mathfrak{A}}$ is a canonical isomorphism. □

Proof of Theorem 4.4. For every model $\mathfrak{A}$ of T, $\mathsf{spec}\,\mathfrak{A}$ is an induced subframe of U, and the set $\{\mathsf{spec}\,\mathfrak{A} \mid \mathfrak{A} \models T\}$ covers U, since every qf-type of T is realized in some model of T. It follows from Lemma 5.2 that Tr_U is universal for the equational theory of $\{\mathsf{Tr}_{\mathsf{spec}\,\mathfrak{A}} \mid \mathfrak{A} \models T\}$. But by Theorem 4.5, this is the same as the equational theory of $\{\mathsf{Tr}_{\mathfrak{A}} \mid \mathfrak{A} \models T\}$, since $\mathsf{Tr}_{\mathfrak{A}}$ and $\mathsf{Tr}_{\mathsf{spec}\,\mathfrak{A}}$ are canonically isomorphic. □

The frame U, although universal for trace algebras of Tarskian frames over models of T, is not itself Tarskian. One might ask whether a universal Tarskian frame exists. The answer is yes, provided T is a complete theory: take a qf-saturated model of T (one realizing all qf-types consistent with T). If T is not complete, then the answer is no in general. For example, if T is generated by the single formula $\neg\exists x\ P(x) \vee \neg\exists x\ Q(x)$, then there is a qf-type of T containing $P(x)$ and one containing $Q(x)$, since both are consistent with T, but there is no single model of T containing both these qf-types in its spectrum. However, the answer is again yes if we amend the definition of Tarskian frame to allow disjoint unions of Tarskian frames as defined above. In this case we can take the disjoint union of qf-saturated models, one for each complete extension of T.

6. Relation algebras

Unlike the propositional case, relation and trace algebras of Tarskian frames do not share the same equational theory. Inclusion does hold in one direction: since $\mathsf{Ext} : \mathsf{Tr}_{\mathfrak{A}} \to \mathsf{Rel}_{\mathfrak{A}}$ is a canonical homomorphism, the equational theory of trace algebras is contained in the equational theory of relation algebras of Tarskian frames (and in fact for any class of frames), but not vice versa. Note that Lemma 3.1 does not apply, since the relation algebra on $\mathsf{Traces}_{\mathfrak{A}}$ is not necessarily Tarskian.

The axioms of SKAT proposed in [1] provide some counterexamples for the reverse inclusion:

$$\begin{aligned}
x := d\,;\ y := e &= y := e[x/d]\,;\ x := d \qquad (y \notin \mathsf{FV}(d)),\\
x := d\,;\ y := e &= x := d\,;\ y := e[x/d] \qquad (x \notin \mathsf{FV}(d)),\\
x := d\,;\ x := e &= x := e[x/d],\\
x := e\,;\ \varphi &= \varphi[x/e]\,;\ x := e,\\
x := x &= 1,
\end{aligned}$$

where x and y are distinct variables and $\mathsf{FV}(d)$ denotes the set of variables occurring in d. Special cases are the commutativity conditions

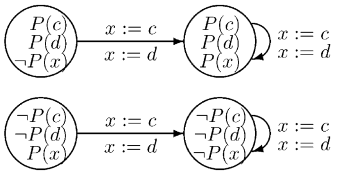
$$\begin{aligned}
x := d\,;\ y := e &= y := e\,;\ x := d \qquad (x \notin \mathsf{FV}(e),\ \ y \notin \mathsf{FV}(d)),\\
\varphi\,;\ x := e &= x := e\,;\ \varphi \qquad (x \notin \mathsf{FV}(\varphi)).
\end{aligned}$$

What is worse, Rel_U is not universal for relation algebras of Tarskian frames, so the analog of Theorem 4.4 for relation algebras does not hold. To see this, consider a signature consisting of constants c, d and unary predicate P. Then

$$[P(c) \leftrightarrow P(d)\,;\ x := c]_U = [P(c) \leftrightarrow P(d)\,;\ x := d]_U, \tag{5}$$

but these two programs are not equivalent in any Tarskian frame in which $c \neq d$. The model U has essentially eight states, depending on the truth values of $P(c)$, $P(d)$,

and $P(x)$. Here is an illustration of relations (5):

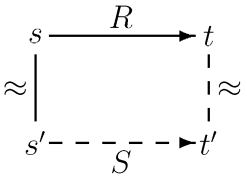


However, note that the two programs of (5) are *observationally equivalent*—indistinguishable by any formula in the language. This indicates that the relation of equality on $\mathsf{Rel}_{\mathfrak{A}}$ is too fine in that it distinguishes programs that are indistinguishable in terms of the preconditions and postconditions satisfied by their input and output states. When we weaken the comparison of input/output relations to observational equivalence, then Rel_U becomes universal.

As with the main results of Section 4, this result follows from more general considerations, so we defer the formal statement and proof until the end of Section 7.

7. More constructions on Kripke frames

Let $\approx$ be an autobisimulation on a Kripke frame K. For binary relations R and S on K, define $R \lesssim S$ if for all s, s', t, if $s \approx s'$ and $(s,t) \in R$, then there exists t' such that $(s',t') \in S$ and $t \approx t'$.



We call the relations R and S *bisimilar* with respect to $\approx$ and write $R \sim S$ if both $R \lesssim S$ and $S \lesssim R$. Let $\mathscr{D}$ be the set of binary relations R such that $R \sim R$.

Lemma 7.1. *The set $\mathscr{D}$ forms a subalgebra of the full relation algebra on K and contains Rel_K as a subalgebra.*

Proof. It is straightforward to show that $\mathscr{D}$ is closed under all the KAT operations. The definition of autobisimulation says exactly that $\mathscr{D}$ contains the generators $[\![\mathsf{p}]\!]_K$, $\mathsf{p} \in \mathsf{P}$ and $[\![\mathsf{b}]\!]_K$, $\mathsf{b} \in \mathsf{B}$ of Rel_K, therefore $\mathscr{D}$ contains all $[\![\mathsf{p}]\!]_K \in \mathsf{Rel}_K$. □

The significance of bisimilarity is that it is a KAT congruence on $\mathscr{D}$, and the quotient algebra $\mathsf{Rel}_K/\sim$ is isomorphic to $\mathsf{Rel}_{K/\approx}$.

Lemma 7.2. *Let* $[\![s]\!] \stackrel{\text{def}}{=} \{t \mid s \approx t\}$. *For* $R \in \mathscr{D}$, *define* $[\![R]\!] \stackrel{\text{def}}{=} \{([\![s]\!], [\![t]\!]) \mid (s,t) \in R\}$. *The map* $[\![\ ]\!]$ *is a* KAT *homomorphism on* $\mathscr{D}$ *and its kernel is the relation* $\sim$. *Restricted to* Rel_K, $[\![\ ]\!]$ *is a canonical homomorphism* $\mathsf{Rel}_K \to \mathsf{Rel}_{K/\approx}$.

Proof. To show that $[\![\ ]\!]$ is a KAT homomorphism on $\mathscr{D}$, it suffices to show that $[\![\bigcup_i A_i]\!] = \bigcup_i [\![A_i]\!]$, $[\![A]\!]\,[\![B]\!] = [\![AB]\!]$, and for $A \subseteq \{(u,u) \mid u \in K\}$, $[\![\{(u,u) \mid u \in K\} - A]\!] = \{(u,u) \mid u \in K\} - [\![A]\!]$. All these arguments are straightforward except for the inclusion $[\![A]\!]\,[\![B]\!] \subseteq [\![AB]\!]$. This is the only place that uses the assumption of membership in $\mathscr{D}$. We argue this case explicitly:

$$
\begin{aligned}
&([\![s]\!], [\![t]\!]) \in [\![A]\!]\,[\![B]\!] \\
&\quad \Rightarrow \exists u\ ([\![s]\!], [\![u]\!]) \in [\![A]\!],\ ([\![u]\!], [\![t]\!]) \in [\![B]\!] \\
&\quad \Rightarrow \exists u, u', u'', s', t''\ (s', u') \in A,\ (u'', t'') \in B,\ u' \approx u \approx u'',\ s \approx s',\ t \approx t'' \\
&\quad \Rightarrow \exists u', u'', s', t'', t'\ (s', u') \in A,\ (u', t') \in B,\ u' \approx u'',\ s \approx s',\ t \approx t'' \approx t' \\
&\qquad \text{since } B \in \mathscr{D} \\
&\quad \Rightarrow \exists s', t'\ (s', t') \in AB,\ s \approx s',\ t \approx t' \\
&\quad \Rightarrow ([\![s]\!], [\![t]\!]) \in [\![AB]\!].
\end{aligned}
$$

To show that $[\![\ ]\!]$ is canonical on Rel_K, it suffices to show that it acts canonically on atomic symbols; that is, $[\![[\![\mathsf{p}]\!]_K]\!] = [\![\mathsf{p}]\!]_{K/\approx}$ and $[\![[\![\mathsf{b}]\!]_K]\!] = [\![\mathsf{b}]\!]_{K/\approx}$. These properties are immediate from the definition of $K/\!\approx$.

Finally, to show that $\sim$ on $\mathscr{D}$ is the kernel of $[\![\ ]\!]$, it suffices to argue that

$$R \lesssim S \Leftrightarrow \{([\![s]\!], [\![t]\!]) \mid (s,t) \in R\} \subseteq \{([\![s]\!], [\![t]\!]) \mid (s,t) \in S\}.$$

The left-hand side and right-hand side are equivalent to

(i) $\forall s\ \forall s'\ \forall t\ s \approx s' \wedge (s,t) \in R \Rightarrow \exists t'\ t \approx t'$, and $(s',t') \in S$,
(ii) $\forall s\ \forall t\ (s,t) \in R \Rightarrow \exists s'\ \exists t'\ s \approx s' \wedge t \approx t'$ and $(s',t') \in S$,

respectively. Now (i) implies (ii) by taking $s' = s$. For the converse, suppose $s \approx s'$ and $(s,t) \in R$. By (ii), there exist s'', t'' such that $s \approx s''$, $t \approx t''$, and $(s'', t'') \in S$. Since $S \in \mathscr{D}$, $S \sim S$, and $s' \approx s \approx s''$, therefore there exists t' such that $(s',t') \in S$ and $t' \approx t'' \approx t$. □

Combining (1) and Lemmas 5.4 and 7.2, we have the following commutative diagram that captures a fundamental relationship between trace and relation algebras:

$$
\begin{array}{ccc}
\mathsf{Tr}_K & \xrightarrow{\ \mathsf{Ext}\ } & \mathsf{Rel}_K \\
{\scriptstyle [\![\ ]\!]^{-1}}\uparrow & & \downarrow{\scriptstyle [\![\ ]\!]} \\
\mathsf{Tr}_{K/\approx} & \xrightarrow[\ \mathsf{Ext}\ ]{} & \mathsf{Rel}_{K/\approx}
\end{array}
\tag{6}
$$

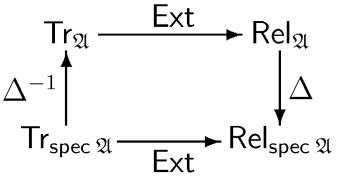
The arrow labeled $[\![\ ]\!]^{-1}$ is an isomorphism by Lemmas 5.3 and 5.4. The diagram commutes because all the homomorphisms in question are canonical.

We say that terms p and q are *observationally equivalent* over $\mathfrak{A}$ if $[\![\mathsf{p}]\!]_{\mathfrak{A}}$ and $[\![\mathsf{q}]\!]_{\mathfrak{A}}$ are bisimilar with respect to the autobisimulation $s \approx t \stackrel{\text{def}}{\Leftrightarrow} \Delta(s) = \Delta(t)$ on the Tarskian frame $K_{\mathfrak{A}}$. In other words, if $\Delta(s) = \Delta(s')$ and $(s,t) \in [\![\mathsf{p}]\!]_{\mathfrak{A}}$, then there exists t' such that $(s',t') \in [\![\mathsf{q}]\!]_{\mathfrak{A}}$ and $\Delta(t) = \Delta(t')$, and vice versa.

The following is our main result on relation algebras.

Theorem 7.3. *The algebra* Rel_U *is universal for the equational theory of relation algebras of Tarskian frames over models of* T *modulo observational equivalence. In other words,* $[\![\mathsf{p}]\!]_U = [\![\mathsf{q}]\!]_U$ *iff* p *and* q *are observationally equivalent over all models of* T.

Proof. In the special case of the autobisimulation $s \approx t \stackrel{\text{def}}{\Leftrightarrow} \Delta(s) = \Delta(t)$, diagram (6) takes the form



By Lemma 7.2, p and q are observationally equivalent over $\mathfrak{A}$ iff $[\![\mathsf{p}]\!]_{\mathfrak{A}}$ and $[\![\mathsf{q}]\!]_{\mathfrak{A}}$ have the same image under Δ, which occurs iff $[\![\mathsf{p}]\!]_{\mathsf{spec}\,\mathfrak{A}} = [\![\mathsf{q}]\!]_{\mathsf{spec}\,\mathfrak{A}}$. But by Lemma 5.2, Rel_U is universal for the equational theory of $\mathsf{Rel}_{\mathsf{spec}\,\mathfrak{A}}$ for $\mathfrak{A} \models T$. Thus $[\![\mathsf{p}]\!]_U = [\![\mathsf{q}]\!]_U$ iff $[\![\mathsf{p}]\!]_{\mathsf{spec}\,\mathfrak{A}} = [\![\mathsf{q}]\!]_{\mathsf{spec}\,\mathfrak{A}}$ over all $\mathfrak{A} \models T$ iff p and q are observationally equivalent over all models of T. □

Can one capture the equational theory of relation algebras of Tarskian frames in a Tarskian frame? As with trace algebras, the answer is yes, provided we allow disjoint unions of Tarskian frames: take the disjoint union of sufficiently many Tarskian frames, where "sufficiently many" means that if there exists $\mathfrak{A}$ such that $[\![\mathsf{p}]\!]_{\mathfrak{A}} \neq [\![\mathsf{q}]\!]_{\mathfrak{A}}$, then there is at least one such frame in the class taken.

Acknowledgements

This work was supported in part by NSF Grant CCR-0105586 and by ONR Grant N00014-01-1-0968. The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of these organizations or the US Government.

References

[1] A. Angus, D. Kozen, Kleene algebra with tests and program schematology, Tech. Rep. 2001-1844, Computer Science Department, Cornell University, July 2001.
[2] A. Barth, D. Kozen, Equational verification of cache blocking in LU decomposition using Kleene algebra with tests, Tech. Rep. 2002-1865, Computer Science Department, Cornell University, June 2002.
[3] J.L. Bell, A.B. Slomson, Models and Ultraproducts, North-Holland, Amsterdam, 1971.
[4] C.C. Chang, H.J. Keisler, Model Theory, North-Holland, Amsterdam, 1973.
[5] C. Hardin, D. Kozen, On the elimination of hypotheses in Kleene algebra with tests, Tech. Rep. 2002-1879, Computer Science Department, Cornell University, October 2002.
[6] D. Harel, D. Kozen, J. Tiuryn, Dynamic Logic, MIT Press, Cambridge, MA, 2000.
[7] D.M. Kaplan, Regular expressions and the equivalence of programs, J. Comput. System Sci. 3 (1969) 361–386.
[8] D. Kozen, A completeness theorem for Kleene algebras and the algebra of regular events, Inform. and Comput. 110 (2) (1994) 366–390.
[9] D. Kozen, Kleene algebra with tests, Trans. Programming Languages Systems 19 (3) (1997) 427–443.
[10] D. Kozen, On Hoare logic and Kleene algebra with tests, Trans. Comput. Logic 1 (1) (2000) 60–76.
[11] D. Kozen, Automata on guarded strings and applications, Tech. Rep. 2001-1833, Computer Science Department, Cornell University, January 2001.
[12] D. Kozen, Halting and equivalence of schemes over recursive theories, Tech. Rep. 2002-1881, Computer Science Department, Cornell University, October 2002.
[13] D. Kozen, M.-C. Patron, Certification of compiler optimizations using Kleene algebra with tests, in: J. Lloyd, V. Dahl, U. Furbach, M. Kerber, K.-K. Lau, C. Palamidessi, L.M. Pereira, Y. Sagiv, P.J. Stuckey (Eds.), Proc. first Internat. Conf. Computational Logic (CL2000), Lecture Notes in Artificial Intelligence, Vol. 1861, Springer, London, 2000, pp. 568–582.
[14] D. Kozen, F. Smith, Kleene algebra with tests: completeness and decidability, in: D. van Dalen, M. Bezem (Eds.), Proc. 10th Internatat. Workshop Computer Science Logic (CSL'96), Lecture Notes in Computer Science, vol. 1258, Springer, Utrecht, The Netherlands, 1996, pp. 244–259.
[15] D. Kozen, J. Tiuryn, Intuitionistic linear logic and partial correctness, in: Proc. 16th Symp. Logic in Computer Science (LICS'01), IEEE, New York, 2001, pp. 259–268.
[16] V.R. Pratt, Dynamic algebras and the nature of induction, in: Proc. 12th Symp. Theory of Computer, ACM, New York, 1980, pp. 22–28.